

AFFIDAVIT

I, Jarred A. Payne, am a Task Force Officer (“TFO”) with the Federal Bureau of Investigation (“FBI”) being duly sworn, depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I have been employed as a law enforcement officer with the Kanawha County, West Virginia Sheriff’s Office since February 2017. Prior to employment at the Kanawha County Sheriff’s Office, I was employed as a Police Officer in West Virginia from 2009-2017. I am currently assigned to the FBI as a Task Force Officer. While assigned to the FBI, I have investigated federal criminal violations related to high technology or cybercrime, child exploitation, and child pornography. I have gained experience through training at FBI’s Child Exploitation Unit, the United States Secret Service’s National Computer Forensics Institute, the National White Collar Crime Center, Fox Valley Technical College, the West Virginia State Police Academy, and everyday work relating to conducting these types of investigations. I have received training in the area of child pornography and child exploitation, and have had the opportunity to observe and review numerous examples of child pornography (as defined in 18 U.S.C. § 2256) in all forms of media including computer media. I have investigated hundreds of cases involving child pornography and child exploitation both in the State of West Virginia and through various Federal investigations. I am a certified Digital Evidence Extraction Technician (DEXT) and Computer Analysis Response Team (CART) Technician through the FBI and received specialized training and certification through the FBI for those, both in Quantico, Virginia. Moreover, I am a deputized federal law enforcement officer who is engaged in enforcing the criminal laws, including 18 U.S.C. § 2423, and I am authorized by law to request a search warrant.

2. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant authorizing the examination of property—a black Motorola cell phone, model MC38D, as further described below and in Attachment A—which is currently in law enforcement possession, and the extraction from that property of electronically stored information described in Attachment B.

3. This affidavit is intended to show only that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter. The probable cause statement is based upon information of which I am personally aware as well as information that has been conveyed to me by other law enforcement officers.

IDENTIFICATION OF THE DEVICES TO BE EXAMINED

4. The property to be searched includes the contents of one electronic device (“the Device”): a black Motorola cell phone, model MC38D.

5. The Device is presently in the possession of the Kanawha County Sheriff’s Department, 301 Virginia Street East, Charleston, WV 25301. The Device was lawfully seized from Jon Pieter Vanbreemen’s (“VANBREEMEN”) person on May 9, 2023, pursuant to arrest on West Virginia state charges. Upon information and belief, the Device has been maintained in such a manner that it is in the same condition as at the time it was seized.

6. The applied-for warrant would authorize the forensic examination of the Device for the purpose of identifying electronically stored data particularly described in Attachment B.

STATUTES UNDER INVESTIGATION

7. VANBREEMEN is currently under indictment for violations of Title 18, United States Code, Sections 2423(b) (travel to engage in illicit sexual activity with a minor) and 2423(e) (attempt to travel to engage in illicit sexual activity with a minor). Additional evidence

provides probable cause to believe that defendant committed offenses under 18 U.S.C. § 2252A (possessing, receiving, and distributing child pornography). I seek to search the Device to locate evidence of criminal violations set forth above for items specified in Attachment B, incorporated herein by reference.

PROBABLE CAUSE

8. On or about May 7, 2023, a law enforcement officer was acting in an undercover capacity (“UCO”). In that role, the UCO had created a profile on a social media application that could be accessed either by computer or cell phone. The UCO was portraying a mother of two girls, ages 11 and 13. The UCO created a post on the application that read, “bored momma bear looking for like minded fun....”

9. That same date, the UCO was contacted by a user on the application who was later identified as JON PIETER VANBREEMEN, age 41, of Covington, Virginia.

10. In his initial messages to the UCO on the application, VANBREEMEN stated that he was “very interested for sure.” VANBREEMEN quickly brought up meeting in person with the UCO, advising that he lived close by in Covington, Virginia.

11. During the conversation, VANBREEMEN confirmed that he was seeking intimacy with the UCO and her daughters. When inquiring as to the girls’ experience with oral sex, he stated, “There is nothing hotter than a girl orgasm...Well a few things ;).” The UCO confirmed that the 11-year-old had given and received oral sex, to which VANBREEMEN responded, “That is good. Never like to see them miss the pleasure they should get.”

12. The following day, May 8, 2023, VANBREEMEN had a phone conversation with the UCO and her purported 13-year-old daughter where he told the child that he would be there tomorrow for a visit. During the phone conversation, the UCO confirmed that VANBREEMEN

was “on the same page” as her. VANBREEMEN advised that he was, and that he was up for whatever the girls wanted to do.

13. On May 9, 2023, VANBREEMEN messaged the UCO about meeting at a restaurant in White Sulphur Springs. That same date, VANBREEMEN drove from Covington, Virginia to White Sulphur Springs, West Virginia to meet with the UCO.

14. During the meeting at the restaurant, the UCO asked VANBREEMEN if the girls were too young for him. He advised the UCO they were “right on the line” and that his “line” was 11 years old. VANBREEMEN stated that he had groomed and sexually abused an 11-year-old girl previously, including having sexual intercourse with her.

15. After VANBREEMEN and the UCO finished at the restaurant, they began the walk to where VANBREEMEN understood the girls to be. While walking, VANBREEMEN was placed under arrest. At the time of his arrest, the Device was seized as part of a search incident to arrest. Since that time, the data on the Device has been preserved and the contents of the Device have not been reviewed by law enforcement.

16. In VANBREEMEN’s post arrest interview, he stated that he had received child pornography on several occasions. He also noted that he “traded” what he described as child erotica “every couple of days” on platforms including Redditt and Wickr. Moreover, VANBREEMEN stated that he understood the post to mean intimacy with the mother and her girls even though it was not explicit.

CHARACTERISTICS OF CHILD PORNOGRAPHY COLLECTORS

17. Based on my training, I am aware that the following characteristics are common to individuals who trade in child pornography:

- a. Individuals who possess and/or distribute child pornography may receive sexual gratification, stimulation, and satisfaction from contact with children, or from fantasies they may have viewing children engaged in sexual activity, sexually suggestive poses, or from literature describing such activity;
- b. Individuals who possess, and/or distribute child pornography may collect sexually explicit or sexually suggestive material depicting children, in a variety of media, including photographs, magazines, motion pictures, videotapes, books, slides and/or drawings or other visual media. These individuals often maintain this material for sexual arousal and gratification. Furthermore, they may use this material to lower the inhibitions of children they are attempting to seduce, to arouse a child partner, or to demonstrate the desired sexual acts;
- c. Individuals who possess, and/or distribute child pornography often possess and maintain copies of child pornographic material, including but not limited to pictures, films, video tapes, magazines, negatives, photographs, correspondence, mailing lists, books, and tape recordings, in the privacy and security of their home. Prior investigations into these offenses have shown that child pornography offenders typically retain pictures, films, photographs, negatives, magazines, correspondence, books, tape recordings, mailing lists, child erotica, and videotapes for many years;
- d. Individuals who possess, and/or distribute child pornography often begin their child pornography collections by obtaining child abuse material through various free avenues afforded by the Internet, like P2P file sharing. Thereafter, these individuals may escalate their activities by producing and/or distributing child pornography, for the purpose of trading this material to add to their own child pornography collection;
- e. Individuals who possess, and/or distribute child pornography often maintain their digital or electronic collections in a safe, secure and private environment, such as a computer, Smartphone or surrounding area. These collections are often maintained for several years and are maintained on multiple devices, to afford immediate access to view the material;
- f. Individuals who possess, and/or distribute child pornography may correspond with others to share information and material, and rarely destroy this correspondence. These individuals often maintain lists of names, email addresses and telephone numbers of others with whom they have been in contact regarding their shared interests in child pornography.

**SPECIFICS OF SEARCH AND SEIZURE OF COMPUTER
AND ELECTRONIC DEVICE SYSTEMS**

18. Based upon my training and experience and information related to me by agents and others involved in the forensic examination of computers and other electronic devices, I know that data can be stored on a variety of computer systems and storage devices, including external and internal hard drives, flash drives, thumb drives, micro SD cards, macro SD cards, DVDs, gaming systems, SIM cards, cellular phones capable of storage, floppy disks, compact disks, magnetic tapes, memory cards, memory chips, and online or offsite storage servers maintained by corporations, including but not limited to “cloud” storage.

19. As is the case with most digital technology, communications by way of computer or cellular phone can be saved or stored on the computer used for these purposes. Storing this information can be intentional, i.e., by saving an e-mail as file on the computer or saving the location of one’s favorite websites in, for example, “bookmarked” files. Digital information can also be retained unintentionally, e.g., traces of the path of an electronic communication may be automatically stored in many places (e.g., temporary files or ISP client software, among others). In addition to electronic communications, a computer user’s Internet activities generally leave traces or “footprints” in the web cache and history files of the browser used.

20. I submit that there is probable cause to believe the items in Attachment B will be stored on the Device for at least the following reasons:

- a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the

storage medium that can reveal information such as online nicknames and passwords. Operating systems can record the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.

- b. Information stored within a computer and other electronic storage media may provide crucial evidence of the “who, what, why, when, where, and how” of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within a computer or storage media (e.g., registry information, communications, images and movies, transactional information, records of session times and durations, Internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the computer or storage media. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence.
- c. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed, thus inculpating or exculpating the computer owner.
- d. Moreover, information stored within a computer and other electronic storage media may provide relevant insight into the device user’s state of mind as it relates to the offense under investigation. For example, information within the device may indicate the owner’s motive and intent to commit a crime (e.g., internet searches indicating criminal planning), or consciousness of guilt (e.g., running a “wiping” program to destroy evidence on the device or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).
- e. A person with appropriate familiarity with how a computer or electronic device system works can, after examining this forensic evidence in its proper context, draw conclusions about how the device was used, the purpose of its use, who used it, and when.
- f. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer or electronic device system evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on such a device is evidence may depend on other information stored on the device and the application of knowledge about how a device behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

- g. Further, in finding evidence of how a computer or electronic device system was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.
- h. I know that when an individual uses a computer or electronic device system to distribute or attempt to distribute child pornography, the individual's device will generally serve both as an instrumentality for committing the crime and also as a storage medium for evidence of the crime. The device is an instrumentality of the crime because it is used as a means of committing the criminal offense. The device is also likely to be a storage medium for evidence of a crime. From my training and experience, I believe that a device used to commit a crime of this type may contain: data that is evidence of how the device was used; data that was sent or received; notes as to how the criminal conduct was achieved; records of Internet discussions about the crime; and other records that indicate the nature of the offense.

FORENSIC ANALYSIS

21. Based on the foregoing, and consistent with Federal Rule of Criminal Procedure 41(e)(2)(B), the warrant I am applying for would permit the examination of the Device consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the Device to human inspection in order to determine whether it is evidence described by the warrant. If the Device has been locked using a passcode, the examination may also include the use of computer programs or other devices to bypass the passcode or otherwise access the material located on the Device.

22. *Manner of execution.* Because this warrant seeks only permission to examine devices already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

CONCLUSION

23. I submit that this affidavit supports probable cause for a search warrant authorizing the examination of the Device described in Attachment A to seek the items described in Attachment B.

24. Moreover, I am aware that the recovery of data by a computer forensic analyst takes significant time; much the way recovery of narcotics must later be forensically evaluated in a lab, digital evidence will also undergo a similar process. For this reason, unless otherwise ordered by the Court, the return will not include the specific evidence later examined by a forensic analyst.

Further your Affiant sayeth naught.


DETECTIVE FARRED PAYNE
KANAWHA COUNTY SHERIFF'S OFFICE

Sworn to by the Affiant telephonically in accordance with the procedures of Rule 4.1 this
29th day of June, 2023.


OMAR J. ABOULHOSN
UNITED STATES MAGISTRATE JUDGE
SOUTHERN DISTRICT OF WEST VIRGINIA